

jc997 U.S. PTO  
10/058834  
01/30/02

PATENT  
ATTORNEY DOCKET NO. 0074/019001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants : Kazuhiro KOYAMA et al. Art Unit:  
Serial No. : filed concurrently Examiner:  
Filing Date: January 30, 2002  
Title : DATA DISTRIBUTION SYSTEM

Commissioner of Patents and Trademarks  
Washington, D.C. 20231

SUBMISSION OF PRIORITY DOCUMENT

Sir:

Under the provisions of 35 USC 119, applicants hereby claim the benefit of the filing date of Japanese Patent Application No. 2001-39489 filed on February 16, 2001.

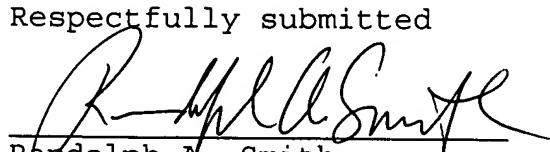
In support of applicants' claim for priority, filed herewith is a certified copy of the priority document in Japanese.

It is respectfully requested that the receipt of the certified copy attached hereto be acknowledged in this application.

If any fees are due in connection with this filing, please charge our Deposit Account No. 19-2586, ref. 0074/019001.

If there are any questions regarding this application, please telephone the undersigned at the telephone number listed below.

Respectfully submitted

  
Randolph A. Smith  
Reg. No. 32,548

Date: January 30, 2002

SMITH PATENT OFFICE  
1901 Pennsylvania Ave., N.W.  
Suite 200  
Washington, D.C. 20006-3433  
Telephone: 202-530-5900  
Facsimile: 202-530-5902  
Koyama013002

日本国特許庁  
JAPAN PATENT OFFICE

JC997 U.S. PRO  
10/058834  
01/30/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application: 2001年 2月16日

出願番号

Application Number: 特願2001-039489

[ST.10/C]:

[JP2001-039489]

出願人

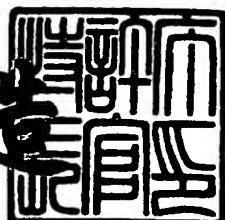
Applicant(s): 松下電器産業株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2002年 1月18日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



【書類名】 特許願  
【整理番号】 2054520199  
【あて先】 特許庁長官殿  
【国際特許分類】 G09C 1/00  
H04L 9/30

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式  
会社内

【氏名】 小山 和宏

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式  
会社内

【氏名】 丹羽 寿男

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式  
会社内

【氏名】 稲垣 哲

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式  
会社内

【氏名】 続木 貴史

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100084364

【弁理士】

【氏名又は名称】 岡本 宜喜

【手数料の表示】

【予納台帳番号】 044336

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9004841

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ配布システム

【特許請求の範囲】

【請求項 1】 データを作成するデータ作成者端末が前記データを利用する利用者端末に前記データを配布する際に、前記データ作成者端末で前記利用者端末での利用可能な項目を規定するための利用制限情報を設定でき、且つ前記利用者端末がデータ作成者端末の許可の下に前記利用制限情報を変更可能とするデータ配布システムであって、

前記データ作成者端末は、

データを作成するデータ作成手段と、

前記利用者端末でのデータの利用条件を設定する利用制限情報設定手段と、

前記利用制限情報設定手段で設定した利用制限情報に基づいて、前記データを配布形式データへ変換する第1の変換手段と、

前記利用者端末と通信を行なう第1の通信手段と、

一度設定した利用条件を前記利用者端末からの要求によって変更する際に、前記利用者端末から送信された利用情報変更要求が、正当な利用者端末からの送信であるか否かを確認する第1の判定手段と、を具備し、

前記利用者端末は、

前記データ作成者端末とデータ通信を行う第2の通信手段と、

前記データ作成者端末より送信された前記配布形式データを記録する記憶媒体と、

前記記憶媒体にデータを入出力する記憶媒体インターフェースと、

前記記憶媒体に保持された前記配布形式データを利用するために入力する利用項目入力手段と、

前記利用者端末の利用者に関する情報を入力する利用者情報入力手段と、

前記記憶媒体に保持された前記配布形式データから利用制限情報を取り出す利用制限情報取得手段と、

前記利用制限情報、前記利用項目、前記利用者情報を基に、前記配布形式デー

タに対する前記利用者端末での利用項目の実行の可否を判定する第2の判定手段と、

前記第2の判定手段の結果を基に、前記配布形式データに対する前記利用項目を実行する利用処理手段と、

前記データ作成者端末に対して利用制限情報の変更要求を入力する変更要求入力手段と、

前記変更要求入力手段で入力された変更要求をデータ作成者端末に送信可能な形式に変換する第2の変換手段と、

前記変更要求が前記データ作成者端末に認められた場合に、前記変更要求を前記記憶媒体上の前記配布形式データに反映させる利用制限情報書換手段と、を具備することを特徴とするデータ配布システム。

【請求項2】 前記データ作成者端末は、

前記第1の変換手段の処理として、前記配布形式データを作成する際に、前記配布形式データを一意に定めるためのデータ識別情報を収めるステップと、前記データを共通鍵暗号方式で暗号化するための共通鍵1で暗号化し、前記配布形式データに収めるステップと、前記利用制限情報を前記配布形式データに収めるステップと、利用制限情報のハッシュ値を前記配布形式データに収めるステップと、前記共通鍵1を前記配布形式データに収めるステップと、前記配布形式データを公開鍵暗号方式の暗号化の鍵である公開鍵2で暗号化するステップとを含むものであり、

前記利用者端末は、

前記第2の変換手段の処理として、前記変更要求を前記データ作成者端末に送信可能な形式に変換するステップと、前記公開鍵2で暗号化された配布形式データを秘密鍵2で復号するステップを含み、

前記利用制限情報取得手段の処理として、前記利用制限情報をハッシュ変換し、前記配布形式データ中のハッシュ値と比較するステップとを含み、

前記利用処理手段の処理として、暗号化されたデータを共通鍵1で復号するステップを含むものであることを特徴とする請求項1記載のデータ配布システム。

【請求項3】 前記利用制限情報の変更を行う場合のデータ配布システムで

あって、

前記データ作成者端末は、

前記配布データ及び前記利用者端末ごとの利用条件を記録する配布記録データベースと、

前記配布記録データベースとデータの入出力を行う配布記録データベース通信手段と、

前記第1の判定手段により署名が確認された前記変更要求リストを表示する表示手段と、を更に有し、

前記利用者端末は、

前記第2の変換手段の処理として、前記利用制限情報の変更要求と前記利用者情報をまとめて一つの変更要求リストに変換するステップと、前記変更要求リストに署名を行なうステップと、署名が行なわれた前記変更要求リストを公開鍵1で暗号化するステップとを含み、

前記第2の判定手段の処理として、前記データ作成者端末から送信された利用制限情報の変更可否を秘密鍵2によって復号するステップと、前記データ作成者端末から送信された署名を確認するステップとを含み、

前記利用制限情報書換手段の処理として、前記署名の確認後、前記利用制限情報を書き換えるステップを含むものであり、

前記データ作成者端末は、

前記第1の変換手段の処理として、前記利用者端末から送信された前記変更要求リストを秘密鍵1により復号するステップを含み、

前記第1の判定手段の処理として、前記利用者端末から送信された署名を確認するステップを含み、

前記利用制限情報設定手段の処理として、データ利用条件の変更の可否を入力するステップを含み、

前記第1の変換手段の処理として、前記可否の結果に署名を行なうステップと、公開鍵2で暗号化を行なうステップとを含むものであることを特徴とする請求項1又は2記載のデータ配布システム。

【請求項4】 以前に配布された利用者端末に改訂版としてデータを再配布

するための再配布機能を付加したデータ配布システムであって、

前記データ作成者端末は、

前記第1の判定手段の処理として、新たに前記データ作成手段により作成されたデータ及び前記利用制限情報設定手段により設定された利用制限情報が、前記配布記録データベース中の改訂前のデータに存在するか否かを判定するステップを含み、

前記第1の変換手段の処理として、前記第1の判定手段が前記配布記録データベースに改訂前のデータが存在すると判定すれば、前記配布記録データベースの配布記録及び利用制限情報に従って、改訂前のデータと同一の利用条件で改訂版として前記利用者端末に送信用のデータを出力することを特徴とする請求項1～3のいずれか1項記載のデータ配布システム。

【請求項5】 前記利用者端末が配布形式データを再配布した相手である再配布先を前記配布記録データベースに保持する場合のデータ配布システムであつて、

前記利用者端末は、

前記利用項目入力手段の処理として、再配布先を入力するステップを含み、

前記第2の変換手段の処理として、前記再配布先と前記利用制限情報取得手段により抽出した前記データ識別情報をまとめて再配布記録データとして作成するステップと、前記再配布記録データに対して公開鍵1で暗号化を行なうステップと、前記再配布記録データに署名を行なうステップとを含み、

前記第2の通信手段の処理として、前記再配布記録データを前記利用者端末に送信するステップを含むものであり、

前記データ作成者端末は、

前記第1の通信手段の処理として、前記再配布記録データを受信するステップを含み、

前記第1の変換手段の処理として、暗号化された再配布記録データを秘密鍵1で復号を行なうステップを含み、

前記第1の判定手段の処理として、前記再配布記録データの署名を確認するステップと、前記再配布記録データを前記配布記録データに追加して前記配布記録

データベースに記録するステップとを含むものであることを特徴とする請求項4記載のデータ配布システム。

【請求項6】 データを作成するデータ作成者端末が前記データを利用する利用者端末に前記データを配布する際に、管理センタはデータの配布記録を保持し、所定の利用者端末に前記データを配布するに際し、前記利用者端末に対して利用制限情報を設定でき、且つ設定された利用制限情報及び配布データを配布記録データとして前記管理センタのセンタデータベースで記録と管理を行い、更に利用者端末から利用制限情報の変更要求があった場合、前記データ作成者端末が利用条件の変更を許可すれば、前記利用者端末に配布されたデータ中の利用制限情報を変更可能とし、且つ変更内容が前記管理センタの前記センタデータベースに記録されるデータ配布システムであって、

前記データ作成者端末は、

データを作成するデータ作成手段と、

前記利用者端末における利用制限情報を設定する利用制限情報設定手段と、

前記データ及び前記利用制限情報を配布形式データに変換する第3の変換手段と、

前記管理センタと通信を行なう第3の通信手段と、

前記利用者端末からの利用制限情報の変更要求が正規の利用者端末から送信されたものか否かを確認する第3の判定手段と、を具備し、

前記管理センタは、

前記データ作成者端末及び前記利用者端末と通信を行なう第4の通信手段と、

前記第4の通信手段を介して受信した前記配布形式データを記録可能な形に変換する第4の変換手段と、

前記配布形式データが配布及び記録可能かを判定すると共に、更に前記利用者端末からの利用制限情報の変更要求の許可が正当な利用者端末からの送信であるか否かを判定する第4の判定手段と、

前記データの前記利用者端末への配布記録、及び前記利用制限情報の改変の記録を保持するセンタデータベースと、

前記センタデータベースにデータの入出力を行うセンタデータベース通信手段

と、を具備し、

前記利用者端末は、

前記管理センタと通信を行う第5の通信手段と、

前記配布形式データを記録する記憶媒体と、

前記記憶媒体にデータの入出力を行う記憶媒体インターフェースと、

前記記憶媒体に保持された前記配布形式データを利用するために入力する利用項目入力手段と、

前記利用者端末の利用者に関する情報を入力する利用者情報入力手段と、

前記記憶媒体に保持された前記配布形式データから利用制限情報を取り出す利用制限情報取得手段と、

前記利用制限情報、前記利用項目、前記利用者情報を基に、前記配布形式データに対する前記利用者端末での利用項目の実行の可否を判定する第5の判定手段と、

前記第5の判定手段の判定結果を基に、前記配布形式データに対する前記利用項目を実行する利用処理手段と、

前記利用制限情報の変更要求を入力する変更要求入力手段と、

前記変更要求入力手段で入力された変更要求を前記管理センタに送信可能な形式に変換する第5の変換手段と、

前記変更要求が前記データ作成者端末に許可された場合に、前記変更要求を前記記憶媒体上の前記配布形式データに反映させる利用制限情報書換手段と、を具備することを特徴とするデータ配布システム。

【請求項7】 前記データ作成者端末は、

前記第3の変換手段の処理として、前記配布形式データを作成する際に、前記配布形式データを一意に定めるためのデータ識別情報を収めるステップと、前記データを共通鍵暗号方式で暗号化するための鍵である共通鍵1で暗号化し、前記配布形式データに収納するステップと、前記共通鍵1を前記配布形式データに収めるステップと、前記利用制限情報を前記配布形式データに収めるステップと、前記利用制限情報のハッシュ値を計算し、前記配布形式データに収めるステップと、前記配布形式データに署名を行なうステップと、前記配布形式データを公開

鍵暗号方式で暗号化するための鍵である公開鍵5で暗号化するステップとを含むものであり、

前記管理センタは、

前記第4の変換手段の処理により、前記公開鍵5で暗号化された配布形式データを復号するための鍵である秘密鍵5によって復号を行なうステップを含み、

前記第4の判定手段の処理により、前記配布形式データの署名を確認するステップと、前記配布形式データから前記利用制限情報をハッシュ変換し、配布形式データ中のハッシュ値と比較するステップとを含み、

前記第4の変換手段の処理により、復号した前記配布形式データを公開鍵暗号方式で暗号化するための鍵である公開鍵2によって暗号化するステップを含み、

前記利用者端末は、

前記第5の変換手段の処理により、前記公開鍵2により暗号化された配布形式データを復号するための鍵である秘密鍵2で復号するステップを含み、

前記利用制限情報取得手段の処理により、配布形式データから前記利用制限情報を取り出すステップと、前記利用制限情報のハッシュ値を計算し、前記配布形式データ中のハッシュ値と比較するステップとを含み、

前記利用処理手段の処理により、暗号化されたデータを前記共通鍵1で復号するステップを含むものであることを特徴とする請求項6記載のデータ配布システム。

【請求項8】 前記利用制限情報の変更を行う場合のデータ配布システムであって、

前記利用者端末は、

前記第5の変換手段の処理により、前記変更要求入力手段からの入力と前記利用者情報入力手段からの入力とを合わせて変更要求リストに変換するステップと、前記変更要求リストに署名を行なうステップと、前記変更要求リストに対して公開鍵5で暗号化を行なうステップとを含み、

前記第5の判定手段の処理により、公開鍵2で暗号化された前記可否の判定結果を秘密鍵2によって復号するステップと、前記判定結果の署名を確認するステップとを含み、

前記利用制限情報書換手段の処理により、署名を確認後、前記利用制限情報を書き換えるステップを含むものであり、

前記管理センタは、

前記第4の変換手段の処理により、受信した変更要求リストを秘密鍵5によつて復号するステップを含み、

前記第4の判定手段の処理により、前記利用者端末から送信された変更要求リストの署名を確認するステップを含み、

前記第4の変換手段の処理により、前記変更要求リストを公開鍵4によって暗号化を行なうステップとを含み、

前記第4の変換手段の処理により、前記公開鍵5で暗号化された可否の判定結果を復号するための鍵である前記秘密鍵5によって復号するステップを含み、

前記第4の判定手段の処理により、前記可否の判定結果の署名を確認するステップを含み、

前記第4の変換手段の処理により、前記可否の判定結果に対して署名を行なうステップと、公開鍵暗号方式で暗号化するための鍵である前記公開鍵2で暗号化するステップを含むものであり、

前記データ作成者端末は、

前記第1の判定手段の処理により署名が確認された前記変更要求リストを表示する表示手段を具備し、

前記第3の変換手段の処理により、秘密鍵4による復号を行なうステップを含み、

前記第3の判定手段の処理により、前記管理センタの署名を確認するステップを含み、

前記利用制限情報設定手段の処理により、前記変更要求の可否を入力するステップを含み、

前記第3の変換手段の処理により、前記可否の判定結果に署名を行なうステップと、公開鍵暗号方式で暗号化するための鍵である前記公開鍵5で暗号化を行なうステップとを更に含むものであることを特徴とする請求項6又は7記載のデータ配布システム。

【請求項9】 以前に配布された利用者端末に改訂版としてデータを再配布するための再配布機能を持たせたデータ配布システムであって、

前記管理センタは、

前記第4の判定手段の処理により、前記配布形式データを前記センタデータベースに改訂前のデータが存在するか否かを判定するステップを含み、

前記第4の変換手段の処理により、前記第4の判定手段が前記センタデータベースに改訂前のデータが存在すると判定すれば、前記配布記録データベースの配布記録及び利用制限情報に従って、改訂前のデータと同一の利用条件で改訂版として前記利用者端末にデータ送信を行うことを特徴とする請求項6～8のいずれか1項記載のデータ配布システム。

【請求項10】 利用者端末が配布形式データを再配布した相手である再配布先を前記配布記録データベースに保持する場合のデータ配布システムであって

前記利用者端末は、

前記利用項目入力手段の処理により、再配布先を入力するステップを含み、

前記第5の変換手段の処理により、前記再配布先と前記利用制限情報取得手段により抽出したデータ識別情報をまとめて再配布記録データとして作成するステップと、前記再配布記録データに対して公開鍵5で暗号化を行なうステップと、前記再配布記録データに署名を行なうステップとを含むものであり、

前記管理センタは、

前記第4の通信手段の処理により、前記再配布記録データを前記データ作成者端末に送信するステップを含み、

前記第4の通信手段の処理により、前記再配布先データを受信するステップを含み、

前記第4の変換手段の処理により、暗号化された再配布記録データを秘密鍵5で復号を行なうステップを含み、

前記第4の判定手段の処理により、前記再配布記録の署名を確認するステップと、前記再配布記録データを前記配布記録データに追加して前記センタデータベースに記録するステップとを含むものであることを特徴とする請求項9記載のデ

ータ配布システム。

【請求項11】 前記利用制限情報は、

各利用者端末ごとに個別に設定可能であり、前記データの表示、再生の可否、複製の作成の可否、複製可能な個数、複製作成が可能な世代数、各世代数ごとの複製作成が可能な個数のうち、1つ以上の情報が設定されたことを特徴とする請求項1～10のいずれか1項記載のデータ配布システム。

【請求項12】 前記利用制限情報は、

表示領域制限情報を含むことを特徴とする請求項1～11のいずれか1項記載のデータ配布システム。

【請求項13】 前記データは、

文章、画像を含む表示可能なデータであり、

前記利用処理手段は、

前記データの閲覧のための表示ステップを含むものであり、

前記表示領域制限情報は、

前記表示装置のサイズ情報、前記表示装置中に表示する前記データの表示倍率情報、利用者端末で非表示とする部分を示す非表示位置情報のうち、1つ以上の情報が設定されたものであることを特徴とする請求項12記載のデータ配布システム。

【請求項14】 前記利用制限情報は、

時間情報を含み、

前記変更要求入力手段は、

前記時間情報を設定するステップを含み、

前記第2の判定手段は、

前記利用者端末で前記データ利用の際に、前記時間情報と利用項目の入力が行なわれた時刻を比較し、利用可否の判定を行なうステップを含むことを特徴とする請求項1～13のいずれか1項記載のデータ配布システム。

【請求項15】 前記管理センタ及び前記データ作成者端末の少なくとも一方は時間計測手段を具備し、

前記第2の通信手段は、

前記第2の判定手段がデータから時間情報を取得した場合、データ利用時に前記管理センタ又は前記データ作成者端末と通信を行ない、前記時間計測手段で計測されている管理時間情報を取得し、

前記第2の判定手段は、

前記時間情報と前記管理時間情報を比較することを特徴とする請求項14記載のデータ配布システム。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、ネットワークを介してデータ配布を行なう際に、利用者ごとの利用条件をきめ細かく設定可能にし、更に設定された利用条件をデータ配布者の許可の下に利用者側が変更可能にしたデータ配布システムに関するものである。

##### 【0002】

##### 【従来の技術】

ディジタルデータの配布に際して、利用者端末での利用条件の制限に関しては、様々な工夫がなされている。例えば特開平10-294726号公報では、電子透かしの手法を用いて著作権情報を著作物に埋め込むことで、著作物の保護を図っている。

##### 【0003】

図9は従来のデータ配布システムにおけるデータ配布側と利用者側との処理手順を示す説明図である。著作物の配布及び利用方法として、ステップ901では各利用者の利用制限情報を、著作権情報として電子透かしの手法により著作物に埋め込む。ステップ902では、著作権情報が埋め込まれた著作物と、著作権情報取り出しのために必要な鍵情報を、ネットワークを経由して利用者端末に提供する。ステップ903では、利用者端末が鍵情報をもとに著作権情報を著作物から取り出す。ステップ904では、著作権情報から利用条件を決定する。ステップ905では、利用者端末で利用したい処理が可能であるか、不可能であるかを判定する。ステップ906では、利用禁止である場合に利用処理を中止し、警告を発する。

【0004】

更に従来の技術として、著作権情報を様々に規定する方法や一度規定された著作権情報を利用者端末側で変更可能とする方法等が示されている。

【0005】

【発明が解決しようとする課題】

しかしながら従来の技術では、データ作成者の許可の下で利用制限情報を変更したい場合には、データ配布側が利用制限情報を電子透かしの手法により埋め込んだ著作物を新たに生成し、利用者端末に新たな著作物を送信しなければならず、非効率的であった。また現在まで提案されている著作権管理システムにおいて、データ作成者の許可の下に利用制限情報を書き換え可能とするシステムを前提にする限り、利用者端末側からの利用制限情報の書き換え要求をデータ作成者側に送信し、この書き換え要求を確実に検証できるようにし、かつ、安全に利用者端末とデータ作成者端末との情報送信を実現する方法は存在しなかった。

【0006】

本発明は、このような従来の問題点に鑑みてなされたものであって、利用者端末での利用条件を詳細に設定できるようにし、かつデータ作成者の許可の下で利用者端末から利用条件を変更できるようにしたデータ配布システムを実現することを目的とする。

【0007】

【課題を解決するための手段】

本願の請求項1の発明は、データを作成するデータ作成者端末が前記データを利用する利用者端末に前記データを配布する際に、前記データ作成者端末で前記利用者端末での利用可能な項目を規定するための利用制限情報を設定でき、且つ前記利用者端末がデータ作成者端末の許可の下に前記利用制限情報を変更可能とするデータ配布システムであって、前記データ作成者端末は、データを作成するデータ作成手段と、前記利用者端末でのデータの利用条件を設定する利用制限情報設定手段と、前記利用制限情報設定手段で設定した利用制限情報に基づいて、前記データを配布形式データへ変換する第1の変換手段と、前記利用者端末と通信を行なう第1の通信手段と、一度設定した利用条件を前記利用者端末からの要

求によって変更する際に、前記利用者端末から送信された利用情報変更要求が、正当な利用者端末からの送信であるか否かを確認する第1の判定手段と、を具備し、前記利用者端末は、前記データ作成者端末とデータ通信を行う第2の通信手段と、前記データ作成者端末より送信された前記配布形式データを記録する記憶媒体と、前記記憶媒体にデータを入出力する記憶媒体インターフェースと、前記記憶媒体に保持された前記配布形式データを利用するために入力する利用項目入力手段と、前記利用者端末の利用者に関する情報を入力する利用者情報入力手段と、前記記憶媒体に保持された前記配布形式データから利用制限情報を取り出す利用制限情報取得手段と、前記利用制限情報、前記利用項目、前記利用者情報を基に、前記配布形式データに対する前記利用者端末での利用項目の実行の可否を判定する第2の判定手段と、前記第2の判定手段の結果を基に、前記配布形式データに対する前記利用項目を実行する利用処理手段と、前記データ作成者端末に対して利用制限情報の変更要求を入力する変更要求入力手段と、前記変更要求入力手段で入力された変更要求をデータ作成者端末に送信可能な形式に変換する第2の変換手段と、前記変更要求が前記データ作成者端末に認められた場合に、前記変更要求を前記記憶媒体上の前記配布形式データに反映させる利用制限情報書換手段と、を具備することを特徴とするものである。

#### 【0008】

本願の請求項2の発明は、請求項1のデータ配布システムにおいて、前記データ作成者端末は、前記第1の変換手段の処理として、前記配布形式データを作成する際に、前記配布形式データを一意に定めるためのデータ識別情報を収めるステップと、前記データを共通鍵暗号方式で暗号化するための共通鍵1で暗号化し、前記配布形式データに収めるステップと、前記利用制限情報を前記配布形式データに収めるステップと、利用制限情報のハッシュ値を前記配布形式データに収めるステップと、前記共通鍵1を前記配布形式データに収めるステップと、前記配布形式データを公開鍵暗号方式の暗号化の鍵である公開鍵2で暗号化するステップとを含むものであり、前記利用者端末は、前記第2の変換手段の処理として、前記変更要求を前記データ作成者端末に送信可能な形式に変換するステップと、前記公開鍵2で暗号化された配布形式データを秘密鍵2で復号するステップを

含み、前記利用制限情報取得手段の処理として、前記利用制限情報をハッシュ変換し、前記配布形式データ中のハッシュ値と比較するステップとを含み、前記利用処理手段の処理として、暗号化されたデータを共通鍵1で復号するステップを含むことを特徴とするものである。

## 【0009】

本願の請求項3の発明は、請求項1又は2のデータ配布システムにおいて、前記利用制限情報の変更を行う場合のデータ配布システムであって、前記データ作成者端末は、前記配布データ及び前記利用者端末ごとの利用条件を記録する配布記録データベースと、前記配布記録データベースとデータの入出力を行う配布記録データベース通信手段と、前記第1の判定手段により署名が確認された前記変更要求リストを表示する表示手段と、を更に有し、前記利用者端末は、前記第2の変換手段の処理として、前記利用制限情報の変更要求と前記利用者情報とをまとめて一つの変更要求リストに変換するステップと、前記変更要求リストに署名を行なうステップと、署名が行なわれた前記変更要求リストを公開鍵1で暗号化するステップとを含み、前記第2の判定手段の処理として、前記データ作成者端末から送信された利用制限情報の変更可否を秘密鍵2によって復号するステップと、前記データ作成者端末から送信された署名を確認するステップとを含み、前記利用制限情報書換手段の処理として、前記署名の確認後、前記利用制限情報を書き換えるステップを含むものであり、前記データ作成者端末は、前記第1の変換手段の処理として、前記利用者端末から送信された前記変更要求リストを秘密鍵1により復号するステップを含み、前記第1の判定手段の処理として、前記利用者端末から送信された署名を確認するステップを含み、前記利用制限情報設定手段の処理として、データ利用条件の変更の可否を入力するステップを含み、前記第1の変換手段の処理として、前記可否の結果に署名を行なうステップと、公開鍵2で暗号化を行なうステップとを含むことを特徴とするものである。

## 【0010】

本願の請求項4の発明は、請求項1～3のいずれか1項のデータ配布システムにおいて、以前に配布された利用者端末に改訂版としてデータを再配布するための再配布機能を附加したデータ配布システムであって、前記データ作成者端末は

、前記第1の判定手段の処理として、新たに前記データ作成手段により作成されたデータ及び前記利用制限情報設定手段により設定された利用制限情報が、前記配布記録データベース中の改訂前のデータに存在するか否かを判定するステップを含み、前記第1の変換手段の処理として、前記第1の判定手段が前記配布記録データベースに改訂前のデータが存在すると判定すれば、前記配布記録データベースの配布記録及び利用制限情報に従って、改訂前のデータと同一の利用条件で改訂版として前記利用者端末に送信用のデータを出力することを特徴とするものである。

## 【0011】

本願の請求項5の発明は、請求項4のデータ配布システムにおいて、前記利用者端末が配布形式データを再配布した相手である再配布先を前記配布記録データベースに保持する場合のデータ配布システムであって、前記利用者端末は、前記利用項目入力手段の処理として、再配布先を入力するステップを含み、前記第2の変換手段の処理として、前記再配布先と前記利用制限情報取得手段により抽出した前記データ識別情報をまとめて再配布記録データとして作成するステップと、前記再配布記録データに対して公開鍵1で暗号化を行なうステップと、前記再配布記録データに署名を行なうステップとを含み、前記第2の通信手段の処理として、前記再配布記録データを前記利用者端末に送信するステップを含むものであり、前記データ作成者端末は、前記第1の通信手段の処理として、前記再配布記録データを受信するステップを含み、前記第1の変換手段の処理として、暗号化された再配布記録データを秘密鍵1で復号を行なうステップを含み、前記第1の判定手段の処理として、前記再配布記録データの署名を確認するステップと、前記再配布記録データを前記配布記録データに追加して前記配布記録データベースに記録するステップとを含むことを特徴とするものである。

## 【0012】

本願の請求項6の発明は、データを作成するデータ作成者端末が前記データを利用する利用者端末に前記データを配布する際に、管理センタはデータの配布記録を保持し、所定の利用者端末に前記データを配布するに際し、前記利用者端末に対して利用制限情報を設定でき、且つ設定された利用制限情報及び配布データ

を配布記録データとして前記管理センタのセンタデータベースで記録と管理を行い、更に利用者端末から利用制限情報の変更要求があった場合、前記データ作成者端末が利用条件の変更を許可すれば、前記利用者端末に配布されたデータ中の利用制限情報を変更可能とし、且つ変更内容が前記管理センタの前記センタデータベースに記録されるデータ配布システムであって、前記データ作成者端末は、データを作成するデータ作成手段と、前記利用者端末における利用制限情報を設定する利用制限情報設定手段と、前記データ及び前記利用制限情報を配布形式データに変換する第3の変換手段と、前記管理センタと通信を行なう第3の通信手段と、前記利用者端末からの利用制限情報の変更要求が正規の利用者端末から送信されたものか否かを確認する第3の判定手段と、を具備し、前記管理センタは、前記データ作成者端末及び前記利用者端末と通信を行なう第4の通信手段と、前記第4の通信手段を介して受信した前記配布形式データを記録可能な形に変換する第4の変換手段と、前記配布形式データが配布及び記録可能かを判定すると共に、更に前記利用者端末からの利用制限情報の変更要求の許可が正当な利用者端末からの送信であるか否かを判定する第4の判定手段と、前記データの前記利用者端末への配布記録、及び前記利用制限情報の改変の記録を保持するセンタデータベースと、前記センタデータベースにデータの入出力を行うセンタデータベース通信手段と、を具備し、前記利用者端末は、前記管理センタと通信を行なう第5の通信手段と、前記配布形式データを記録する記憶媒体と、前記記憶媒体にデータの入出力を行う記憶媒体インターフェースと、前記記憶媒体に保持された前記配布形式データを利用するために入力する利用項目入力手段と、前記利用者端末の利用者に関する情報を入力する利用者情報入力手段と、前記記憶媒体に保持された前記配布形式データから利用制限情報を取り出す利用制限情報取得手段と、前記利用制限情報、前記利用項目、前記利用者情報を基に、前記配布形式データに対する前記利用者端末での利用項目の実行の可否を判定する第5の判定手段と、前記第5の判定手段の判定結果を基に、前記配布形式データに対する前記利用項目を実行する利用処理手段と、前記利用制限情報の変更要求を入力する変更要求入力手段と、前記変更要求入力手段で入力された変更要求を前記管理センタに送信可能な形式に変換する第5の変換手段と、前記変更要求が前記デ

ータ作成者端末に許可された場合に、前記変更要求を前記記憶媒体上の前記配布形式データに反映させる利用制限情報書換手段と、を具備することを特徴とするものである。

## 【0013】

本願の請求項7の発明は、請求項6のデータ配布システムにおいて、前記データ作成者端末は、前記第3の変換手段の処理として、前記配布形式データを作成する際に、前記配布形式データを一意に定めるためのデータ識別情報を収めるステップと、前記データを共通鍵暗号方式で暗号化するための鍵である共通鍵1で暗号化し、前記配布形式データに収納するステップと、前記共通鍵1を前記配布形式データに収めるステップと、前記利用制限情報を前記配布形式データに収めるステップと、前記利用制限情報のハッシュ値を計算し、前記配布形式データに収めるステップと、前記配布形式データに署名を行なうステップと、前記配布形式データを公開鍵暗号方式で暗号化するための鍵である公開鍵5で暗号化するステップとを含むものであり、前記管理センタは、前記第4の変換手段の処理により、前記公開鍵5で暗号化された配布形式データを復号するための鍵である秘密鍵5によって復号を行なうステップを含み、前記第4の判定手段の処理により、前記配布形式データの署名を確認するステップと、前記配布形式データから前記利用制限情報をハッシュ変換し、配布形式データ中のハッシュ値と比較するステップとを含み、前記第4の変換手段の処理により、復号した前記配布形式データを公開鍵暗号方式で暗号化するための鍵である公開鍵2によって暗号化するステップとを含み、前記利用者端末は、前記第5の変換手段の処理により、前記公開鍵2により暗号化された配布形式データを復号するための鍵である秘密鍵2で復号するステップを含み、前記利用制限情報取得手段の処理により、配布形式データから前記利用制限情報を取り出すステップと、前記利用制限情報のハッシュ値を計算し、前記配布形式データ中のハッシュ値と比較するステップとを含み、前記利用処理手段の処理により、暗号化されたデータを前記共通鍵1で復号するステップを含むことを特徴とするものである。

## 【0014】

本願の請求項8の発明は、請求項6又は7のデータ配布システムにおいて、前

記利用制限情報の変更を行う場合のデータ配布システムであって、前記利用者端末は、前記第5の変換手段の処理により、前記変更要求入力手段からの入力と前記利用者情報入力手段からの入力を合わせて変更要求リストに変換するステップと、前記変更要求リストに署名を行なうステップと、前記変更要求リストに対して公開鍵5で暗号化を行なうステップとを含み、前記第5の判定手段の処理により、公開鍵2で暗号化された前記可否の判定結果を秘密鍵2によって復号するステップと、前記判定結果の署名を確認するステップとを含み、前記利用制限情報書換手段の処理により、署名を確認後、前記利用制限情報を書き換えるステップを含むものであり、前記管理センタは、前記第4の変換手段の処理により、受信した変更要求リストを秘密鍵5によって復号するステップを含み、前記第4の判定手段の処理により、前記利用者端末から送信された変更要求リストの署名を確認するステップを含み、前記第4の変換手段の処理により、前記変更要求リストを公開鍵4によって暗号化を行なうステップとを含み、前記第4の変換手段の処理により、前記公開鍵5で暗号化された可否の判定結果を復号するための鍵である前記秘密鍵5によって復号するステップを含み、前記第4の判定手段の処理により、前記可否の判定結果の署名を確認するステップを含み、前記第4の変換手段の処理により、前記可否の判定結果に対して署名を行なうステップと、公開鍵暗号方式で暗号化するための鍵である前記公開鍵2で暗号化するステップを含むものであり、前記データ作成者端末は、前記第1の判定手段の処理により署名が確認された前記変更要求リストを表示する表示手段を具備し、前記第3の変換手段の処理により、秘密鍵4による復号を行なうステップを含み、前記第3の判定手段の処理により、前記管理センタの署名を確認するステップを含み、前記利用制限情報設定手段の処理により、前記変更要求の可否を入力するステップを含み、前記第3の変換手段の処理により、前記可否の判定結果に署名を行なうステップと、公開鍵暗号方式で暗号化するための鍵である前記公開鍵5で暗号化を行なうステップとを更に含むことを特徴とするものである。

## 【0015】

本願の請求項9の発明は、請求項6～8のいずれか1項のデータ配布システムにおいて、以前に配布された利用者端末に改訂版としてデータを再配布するため

の再配布機能を持たせたデータ配布システムであって、前記管理センタは、前記第4の判定手段の処理により、前記配布形式データを前記センタデータベースに改訂前のデータが存在するか否かを判定するステップを含み、前記第4の変換手段の処理により、前記第4の判定手段が前記センタデータベースに改訂前のデータが存在すると判定すれば、前記配布記録データベースの配布記録及び利用制限情報に従って、改訂前のデータと同一の利用条件で改訂版として前記利用者端末にデータ送信を行うことを特徴とするものである。

【0016】

本願の請求項10の発明は、請求項9のデータ配布システムにおいて、利用者端末が配布形式データを再配布した相手である再配布先を前記配布記録データベースに保持する場合のデータ配布システムであって、前記利用者端末は、前記利用項目入力手段の処理により、再配布先を入力するステップを含み、前記第5の変換手段の処理により、前記再配布先と前記利用制限情報取得手段により抽出したデータ識別情報をまとめて再配布記録データとして作成するステップと、前記再配布記録データに対して公開鍵5で暗号化を行なうステップと、前記再配布記録データに署名を行なうステップとを含むものであり、前記管理センタは、前記第4の通信手段の処理により、前記再配布記録データを前記データ作成者端末に送信するステップを含み、前記第4の通信手段の処理により、前記再配布先データを受信するステップを含み、前記第4の変換手段の処理により、暗号化された再配布記録データを秘密鍵5で復号を行なうステップを含み、前記第4の判定手段の処理により、前記再配布記録の署名を確認するステップと、前記再配布記録データを前記配布記録データに追加して前記センタデータベースに記録するステップとを含むことを特徴とするものである。

【0017】

本願の請求項11の発明は、請求項1～10のいずれか1項のデータ配布システムにおいて、前記利用制限情報は、各利用者端末ごとに個別に設定可能であり、前記データの表示、再生の可否、複製の作成の可否、複製可能な個数、複製作成が可能な世代数、各世代数ごとの複製作成が可能な個数のうち、1つ以上の情報が設定されたことを特徴とするものである。

【0018】

本願の請求項12の発明は、請求項1～11のいずれか1項のデータ配布システムにおいて、前記利用制限情報は、表示領域制限情報を含むことを特徴とするものである。

【0019】

本願の請求項13の発明は、請求項12のデータ配布システムにおいて、前記データは、文章、画像を含む表示可能なデータであり、前記利用処理手段は、前記データの閲覧のための表示ステップを含むものであり、前記表示領域制限情報は、前記表示装置のサイズ情報、前記表示装置中に表示する前記データの表示倍率情報、利用者端末で非表示とする部分を示す非表示位置情報のうち、1つ以上の情報が設定されたことを特徴とするものである。

【0020】

本願の請求項14の発明は、請求項1～13のいずれか1項のデータ配布システムにおいて、前記利用制限情報は、時間情報を含み、前記変更要求入力手段は、前記時間情報を設定するステップを含み、前記第2の判定手段は、前記利用者端末で前記データ利用の際に、前記時間情報と利用項目の入力が行なわれた時刻を比較し、利用可否の判定を行なうステップを含むことを特徴とするものである。

【0021】

本願の請求項15の発明は、請求項14のデータ配布システムにおいて、前記管理センタ及び前記データ作成者端末の少なくとも一方は時間計測手段を具備し、前記第2の通信手段は、前記第2の判定手段がデータから時間情報を取得した場合、データ利用時に前記管理センタ又は前記データ作成者端末と通信を行ない、前記時間計測手段で計測されている管理時間情報を取得し、前記第2の判定手段は、前記時間情報と前記管理時間情報を比較することを特徴とするものである。

【0022】

【発明の実施の形態】

本発明のデータ配布システムに関する説明をする前に、暗号技術、署名技術、

ハッシュ変換について説明する。暗号技術には共通鍵暗号方式と公開鍵暗号方式とがある。共通鍵暗号方式は、暗号化と復号と同じ暗号化鍵を使用する暗号方式である。共通鍵暗号方式は、公開鍵暗号に比較して高速に暗号化及び復号を行なえる反面、事前に暗号化側と復号側で共通の暗号化鍵を保持しなければならず、共通の鍵を保持する過程で共通鍵が露呈してしまう危険性がある。

## 【0023】

一方、公開鍵暗号方式は、情報の暗号化を公開鍵で行い、復号を秘密鍵と呼ばれる鍵で行なうことを特徴とする。よって、データを受信する側は一対の公開鍵と秘密鍵を生成し、公開鍵を一般に公開することが可能となる。データを送信する側は、公開されている公開鍵を用いてデータを暗号化し、受信側に送ることができる。このため、公開鍵暗号方式は、共通鍵暗号方式に比較して、データの復号に必要な秘密鍵が露呈してしまう危険性が少ないと見える。

## 【0024】

次に署名技術について説明する。署名技術は公開鍵暗号方式に使用する秘密鍵を用いてデータ変換を行なう方式である。署名を行なったデータを送信しようとする者は、自身の秘密鍵を用いて送信したいデータを変換する。受信者は、署名が行なわれたデータを受信すると、公開鍵を用いてデータの変換を行なう。このとき、正しいデータが得られれば署名は正しいものと判断できる。これは、データ送信者のみが秘密鍵を知っているために可能となる技術である。

## 【0025】

次にハッシュ変換について説明する。ハッシュ変換はデータに対して一定サイズのランダム性の高い変換結果を生成する一方向性の変換である。あるデータのハッシュ変換の結果と同一の変換結果が、異なるデータに対する同一のハッシュ変換から得られないという特徴を有する。

## 【0026】

## (実施の形態1)

以下に本発明の実施の形態1におけるデータ配布システムについて、図面を参照しつつ説明する。本実施の形態のデータ配布システムは、そのハードウェアとしてデータ作成者端末101と利用者端末201により構成される。図1はデ

ータ作成者端末101の構成図である。このデータ作成者端末101はデータを作成する機能と、作成したデータを利用者へ配布する機能とを有する。

## 【0027】

図2は利用者端末201の構成図である。利用者端末201は配布されたデータを利用者が利用するための端末である。データ作成者端末101から利用者端末201へ配布される配布形式データ301の構成例を図3に示す。

## 【0028】

図1のデータ作成者端末101において、データ作成手段102は配布すべき元データを作成する手段である。利用制限情報設定手段103は元データに対して、配布する利用者端末201ごとに利用制限情報303を設定する手段である。変換手段104は作成された元データを配布形式データ301に変換する第1の変換手段である。配布記録データベース105は配布記録を保持するデータベースである。配布記録データベース通信手段106は配布記録データベース105とデータ通信を行なうための手段である。

## 【0029】

判定手段108は利用者端末201から送られた変更要求の正当性を判定する第1の判定手段である。通信手段107はネットワーク109と接続され、利用者端末201と通信を行う第1の通信手段である。表示手段110は利用者端末201から送られた利用制限情報303の変更要求に関する情報を表示する手段である。

## 【0030】

図2に示す利用者端末201は、配布形式データ301を利用するためネットワーク109を介してデータ作成者端末101に接続される。利用者端末201において、通信手段202は図1のデータ作成端末101と通信する第2の通信手段である。記憶媒体203は通信手段202によって受信した配布形式データ301を保持する記憶媒体である。記憶媒体インターフェース204は記憶媒体203にデータを入出力するためのインターフェースである。

## 【0031】

利用制限情報取得手段205は記憶媒体203に保持された配布形式データ3

01から記憶媒体インターフェース204を介して利用制限情報303を取得する手段である。利用項目入力手段206は利用項目を入力する入力手段である。利用者情報入力手段207は利用者端末201の利用者に関する情報を入力する入力手段である。判定手段208は、利用制限情報取得手段205、利用項目入力手段206、及び利用者情報入力手段207からの入力結果から、利用者が配布形式データ301を利用可能であるか否かを判定する第2の判定手段である。

#### 【0032】

利用処理手段209は判定手段208によって利用可能であると判定されたとき、元データを利用するための処理を行う手段である。変更要求入力手段210は利用制限情報303を利用者端末201で変更する場合に、変更希望項目を入力する入力手段である。変換手段211は、変更要求入力手段210からの入力、及び利用者情報入力手段207から入力された利用者に関する情報を、例えば1つのファイルに格納するなど、1つのデータとして扱える形式に変換すると共に、データ作成者端末101に送信するための形式である変更要求リストを生成する第2の変換手段である。

#### 【0033】

利用制限情報書換手段212は、変換手段211によって作成された変更要求リストがデータ作成者端末101に許可されたときに、記憶媒体インターフェース204を介して記憶媒体203内の利用制限情報303を書き換える手段である。

#### 【0034】

変換手段211で変更要求リストを作成する手順を図8に示す。変更要求リストの作成手順は、変更要求と利用者情報をまとめて1つのデータ（一体化）にするステップ801と、利用者の署名を行なうステップ802と、公開鍵による暗号化を行なうステップ803とからなる。

#### 【0035】

本実施の形態のデータ配布システムにおいて、データ作成者及び利用者には公開鍵と秘密鍵が予め設定されており、これらの鍵はデータ作成者端末101と利用者端末201とに事前に登録されているものとする。但し、データ作成者と利

用者の公開鍵及び秘密鍵は、必要なときにデータ作成者端末101及び利用者端末201に対して入力するようにしてもよい。なお、本実施の形態では、データ作成者に対して公開鍵1及び秘密鍵1が割り当てられ、利用者に対して公開鍵2及び秘密鍵2が割り当てられているものとする。

## 【0036】

図3は配布形式データ301の構成図であり、データ情報302、利用制限情報303、及びハッシュ値304を有している。利用制限情報303は配布される利用者ごとに設定されるものであり、バージョン情報305、コピー情報306、配布先情報307、データ暗号化鍵308、コピー可能世代数及びコピー可能数309、作成者公開鍵310、作成者連絡先311、利用制限312などから構成される。ハッシュ値304は、利用制限情報303に対して予め設定されたハッシュ変換を施したものである。

## 【0037】

バージョン情報305は配布形式データ301のバージョン情報である。コピー情報306は自身が何代目の何番目のコピーであるかを示す情報であり、例えばデータ作成時は0代目の0個目として示される。配布先情報307は配布先に関する情報である。データ暗号化鍵308は元データを暗号化した際の鍵情報である。コピー可能世代数及びコピー可能数309はコピー可能世代数及びコピー可能数に関する情報である。作成者公開鍵310はデータ作成者端末101の公開鍵（公開鍵1）である。作成者連絡先311はデータ作成者端末101の連絡先である。利用制限312は、元データが動画データであれば再生の可否、複数の曲であれば再生可能な曲番号といった元データの内容ごとに異なるデータである。また、データ情報302には、暗号化されたデータ（以下、暗号化データという）313と、データのタイトル情報などのように暗号化しなくてもよいプレーンテキスト314とが収められている。

## 【0038】

上記のように構成されたデータ配布システムにおいて、データの配布方法について説明する。先ずデータ作成者は図1に示すデータ作成手段102でデータを作成する。利用制限情報設定手段103では、各利用者ごとに利用制限を行なう

ための項目、例えば「データのバージョン：1.0」、「配布者：A」、「コピー：一切禁止」、「閲覧：可」といった情報を設定する。作成されたデータと設定された利用制限情報は変換手段104に送られ、図3に示すような配布形式データ301に変換される。

#### 【0039】

変換手段104は作成された配布形式データ301を更に配布先である利用者ごとの公開鍵2で暗号化する。暗号化された配布形式データ301は配布記録データベース通信手段106に送られ、配布記録データベース105に登録される。またこれと並行して、暗号化された配布形式データ301は配布記録データベース通信手段106から通信手段107に送られ、ネットワーク109を介して利用者端末201へ送信される。

#### 【0040】

図2の利用者端末201の通信手段202で受信され、暗号化された配布形式データ301は変換手段211に出力される。変換手段211は暗号化された配布形式データ301を、予め利用者端末201に設定されている各利用者ごとの秘密鍵2によって復号する。そして判定手段208は利用制限情報303に対してハッシュ変換を行い、ハッシュ値304と比較することで、利用制限情報303が改竄されていないことを確認する。復号された配布形式データ301は記憶媒体インターフェース204を経て記憶媒体203に格納される。

#### 【0041】

利用者端末201の利用者が配布形式データ301を利用するときは、利用項目入力手段206から利用したい項目を入力し、利用者情報入力手段207から利用者に関する情報を入力する。例えば、利用者が利用項目入力手段206から「閲覧」のコマンドを入力し、利用者情報入力手段207から利用者の「パスワード」を入力する。

#### 【0042】

判定手段208は、入力されたパスワードと、利用制限情報取得手段205を介して取り出した利用制限情報303とから、この利用者に対して利用項目が閲覧可能か、又はコピー可能であるかを判断する。判定手段208により利用項目

が利用可能であると判断されれば、利用処理手段209によって利用項目の処理が行なわれる。先ほどの例では、記憶媒体203に格納されている配布形式データ301を記憶媒体インターフェース204を介して取り出し、配布形式データ301内の暗号化データ313を、配布形式データ301内のデータ暗号化鍵308によって復号し、データの表示を行なう。

## 【0043】

また、利用者端末201の利用者が一度設定されている利用制限情報303を変更する場合には、変更要求入力手段210から変更要求を入力し、利用者情報入力手段207から利用者情報を入力する。

## 【0044】

変更要求と利用者情報は図8のステップ801で1つのファイルにまとめられ、データ作成者端末101に送信する形式である変更要求リストに変換される。次のステップ802では、利用者端末201に予め設定されている利用者の公開鍵2によって署名が行なわれる。更に次のステップ803では、データ作成者端末101の公開鍵1により暗号化される。

## 【0045】

暗号化された変更要求リストは通信手段202からネットワーク109を介してデータ作成者端末101に送信される。データ作成者端末101は通信手段107を介して暗号化された変更要求リストを受信し、変換手段104で秘密鍵1により復号を行い、更に判定手段108により署名を確認する。正当なものであれば変更要求リストを表示手段110により表示し、利用制限情報303の変更の許可をデータ作成者に問い合わせる。例えば、利用者がコピーを1世代、1回だけ認めて欲しい場合には、図6に示すような表示内容601が表示される。

## 【0046】

データ作成者は表示を見ながら、変更を許可するか又は許可しないかを利用制限情報設定手段103より入力する。入力結果に対して変換手段104でデータ作成者の署名が行なわれ、利用制限情報303の変更が許可されたか、許可されなかったかを示す変更判定情報に変換される。この変更判定情報は更に変換手段104により、送信先の利用者の公開鍵2で暗号化され、通信手段107によっ

て利用者端末201に送信される。

#### 【0047】

利用者端末201は、暗号化された変更判定情報を受信すると、変換手段211で秘密鍵2を用いて復号し、更に判定手段208によって署名を確認する。署名が正しければ、利用制限情報書換手段212によって、記憶媒体203に格納されている配布形式データ301の利用制限情報303を更新する。

#### 【0048】

データ配布システムにおいて、一度配布したデータを改訂後に再配布したい場合がある。この場合データ作成者端末101のデータ作成手段102から改訂したデータを入力し、利用制限情報設定手段103からバージョン情報305を入力する。このとき判定手段108は配布記録データベース105の内容と比較し、改訂されたデータであるか否かを判断する。改訂されたデータと判断したら、変換手段104は配布記録データベース105に記録されている前回の配布情報と同一の利用者端末201に対して、同一の利用制限情報303を付加して配布形式データ301に変換する。この配布形式データ301は、同一の利用者端末201に配布される。更に再配布の記録は配布記録データベース105に保存される。こうしてデータ作成者端末101は再配布の記録を管理する。

#### 【0049】

一方、利用者端末201において、利用処理手段209が配布形式データ301の複製を作成する際には、利用項目入力手段206から再配布する相手の連絡先を入力する。利用項目入力手段206より入力された再配布を行なう相手の連絡先と、利用制限情報取得手段205により取り出されたバージョン情報305は、再配布情報として1つのファイルにまとめられる。

#### 【0050】

上記の再配布情報は変換手段211により、利用者端末201に予め設定されている利用者の公開鍵2によって署名が行なわれ、データ作成者端末101の公開鍵1により暗号化される。暗号化された再配布情報は通信手段202からデータ作成者端末101に送られる。データ作成者端末101は通信手段107を介して暗号化された再配布情報を受信する。変換手段104で秘密鍵1により復号

を行ない、更に判定手段108により署名を確認する。判定手段108により正規の利用者端末201からの送信であると判断されれば、配布記録データベース通信手段106を介して配布記録データベース105に再配布情報を記録する。

#### 【0051】

さらに、ある利用者端末Aが他の利用者端末Bに配布形式データ301の再々配布を行なう際にも、作成者連絡先311を用いて配布記録データベース105を同様にして更新できる。以上により、データ作成者端末101は、配布形式データ301が何重に再配布されても、改訂データの配布に関して配布記録データベース105を更新することができる。また改訂されたデータを全ての配布形式データ301の保持者に配布できる。

#### 【0052】

##### (実施の形態2)

次に本発明の実施の形態2におけるデータ配布システムについて、図面を参照しつつ説明する。本実施の形態のデータ配布システムは、そのハードウェアとしてデータ作成者端末401と利用者端末201と管理センタ501とにより構成される。図4はデータ作成者端末401の構成図であり、実施の形態1と同一部分は同一の符号を付けて説明する。データ作成者端末401はデータを作成する機能と、作成したデータを利用者へ配布する機能とを有する。図5の管理センタ501はデータの配布記録を管理する機能を有する。本実施の形態のデータ配布システムは、データを管理する管理センタ501が新たに設けられるため、多数のデータ作成者端末401と多数の利用者端末201との間でデータ配布が頻繁に発生する場合に有効なシステムとなる。

#### 【0053】

図4のデータ作成者端末401において、データ作成手段102は配布する元データを作成する手段である。利用制限情報設定手段103は利用者端末201ごとの利用制限情報を設定する手段である。変換手段404は作成した元データを配布形式データ301に変換する第3の変換手段である。通信手段406はネットワーク109に接続され、管理センタ501と通信を行う第3の通信手段である。表示手段110は利用者端末201から送られた利用制限情報303の変

更要求に関する情報を表示する手段である。

#### 【0054】

図5の管理センタ501において、通信手段502はネットワーク109と接続され、データ作成者端末401又は利用者端末201と通信をする第4の通信手段である。変換手段503はデータ作成者端末401のデータ作成手段102から送信された配布形式データ301をセンタデータベース505に記録可能な形式に変換したり、利用者端末201への配布形式に変換する第4の変換手段である。判定手段504は、受信した配布形式データ301が配布可能及び記録可能か否かを判定すると共に、利用者端末201による利用制限情報303の変更要求が、正当な利用者端末からの送信であるか否かを判定する第4の判定手段である。センタデータベース505は配布形式データ301及び配布記録を保持するデータベースである。センタデータベース通信手段506はセンタデータベース505にデータを入出力するための通信手段である。

#### 【0055】

本実施の形態においても、実施の形態1と同様、データ作成者及び利用者には公開鍵と秘密鍵が予め設定されており、これらの鍵はデータ作成者端末401及び利用者端末201に事前に登録されているものとする。本実施の形態では、データ作成者に公開鍵4及び秘密鍵4を割り当て、管理センタ501に対して公開鍵5及び秘密鍵5を割り当て、利用者に対して公開鍵2及び秘密鍵2を割り当てるものとする。但し、データ作成者及び利用者の公開鍵と秘密鍵とは、必要なときにデータ作成者端末401及び利用者端末201に対して入力するようにしてもよい。

#### 【0056】

データ作成者端末401は、実施の形態1と同様にデータ作成手段102を用いて配布データを作成し、利用制限情報設定手段103を用いて利用者端末201で利用制限をする項目を設定する。変換手段404は図1の変換手段104と同様に配布形式データ301に変換する。更に変換手段404は管理センタ501の公開鍵5で配布形式データ301の暗号化を行なう。

#### 【0057】

暗号化された配布形式データ301は通信手段406により、ネットワーク109を介して管理センタ501に送信される。管理センタ501は通信手段502を介して、暗号化された配布形式データ301を受信する。変換手段503は管理センタ501の秘密鍵5を用いて配布形式データ301を復号する。そして判定手段504は署名の内容を確認し、正当なデータ作成者からの配布依頼であることを確認する。

#### 【0058】

判定手段504によって確認された配布形式データ301は、変換手段503によって、利用制限情報303にセンタの連絡先が追加される。そして、予め登録してある利用者端末201の公開鍵2によって暗号化され、通信手段502によって利用者端末201へ送信される。このとき判定手段504は、配布形式データ301及び配布記録をセンタデータベース通信手段506を介してセンタデータベース505に記録する。配布記録は、例えば配布日時など、配布形式データ301の整理や分類に用いる情報である。利用者端末201での配布形式データ301の利用方法は、実施の形態1の場合と同様である。

#### 【0059】

利用者からの利用制限情報303を変更する場合、実施の形態1と同様に利用者端末201は変更要求リストを作成する。変換手段211により作成された変更要求リストは、管理センタ501の公開鍵5で暗号化され、通信手段202によって管理センタ501に送信される。

#### 【0060】

管理センタ501の通信手段502で受信された変更要求リストは、変換手段503で管理センタ501の秘密鍵5で復号され、署名が確認される。署名が確認された変更要求リストは、変換手段503によってデータ作成者の公開鍵4で暗号化される。このとき同時に変更要求リストはセンタデータベース通信手段506を介してセンタデータベース505に記録される。

#### 【0061】

また暗号化された変更要求リストは、データ作成者端末401に送信される。通信手段406により受信された暗号化された変更要求リストは変換手段404

に与えられる。変換手段404はデータ作成者端末401の秘密鍵4により復号し、判定手段405が管理センタ501の署名を確認する。その後、実施の形態1と同様に変更要求が表示手段110に表示され、変更判定情報が作成される。

#### 【0062】

変更判定情報は変換手段404によりデータ作成者の署名が行なわれ、更に管理センタ501の公開鍵5で暗号化された後、管理センタ501へ送信される。管理センタ501は通信手段502を介して変更許可情報を受信する。変換手段503は受信した変更許可情報を秘密鍵5によって復号する。そして判定手段504は変更許可情報の署名を確認し、データ作成者端末401が送信したものであることを確認する。

#### 【0063】

その後、変換手段503は公開鍵2で暗号化を行ない、利用者端末201へ暗号化した変更判定情報の送信を行なう。利用者端末201の変換手段211は、通信手段202を介して受信した変更判定情報を秘密鍵2で復号する。そして判定手段208は変更判定情報の署名を確認する。判定手段208は、署名の確認により管理センタ501からのものであると判断すると、実施の形態1と同様に、利用制限情報書換手段212により配布形式データ301の利用制限情報303を変更する。また、変更結果は管理センタ501のセンタデータベース505及び利用者端末201の記憶媒体203に記録される。

#### 【0064】

データ配布システムにおける利用制限情報303とは、閲覧の禁止、複製の禁止、複製可能な世代数の設定、各複製世代のコピー可能数の設定を示す情報であり、元データの内容により異なる。このような利用制限情報303に、表示領域の制限を行なうための情報を追加する。これにより、例えばデータがテキストデータの場合、元データを加工することなく利用者ごとに表示内容を変更できる。表示領域の制限情報としては、表示画面の大きさ、表示データの拡大率、非表示領域などが考えられる。このような例を図7に示す。図7の例では元データを表示するウインドウの大きさ701と、データの拡大率702及び非表示領域703とを利用制限情報303中のデータとして設定している。例えば同じ表示領域

制限情報を設定すれば、全ての利用者端末で図7と同様の表示となる。なお、これらの利用制限情報を実施の形態1に適用してもよい。

#### 【0065】

更に利用制限情報303に時間情報を付加することもできる。時間情報はアクセスを行なうことが可能な時間を表す。この時間情報は、利用者が利用者端末201を長期間利用しない場合や、配布形式データを一時的に他の利用者に利用させる場合に利用される。時間情報の設定は、利用者が利用項目入力手段206から入力すればよい。設定された時間情報は、利用制限情報書換手段212により、利用制限情報303中、又は配布形式データ301と関連付けられた形で記憶媒体203に記録される。

#### 【0066】

一度、時間情報が設定された配布形式データ301に再度アクセスする際には、判定手段208が時間情報の存在を確認し、管理センタ501に時間情報取得を要求する。このとき管理センタ501から送信される時間情報と設定された時間情報とを比較することで、利用可能か否かを判定できる。また時間情報を管理センタに501に問い合わせる代わりに、利用者端末201内に時刻計測手段を設けてもよい。尚、これらの利用制限情報を実施の形態1に適用してもよい。

#### 【0067】

データ配布システムにおいて、一度配布したデータを改訂後に再配布したい場合、改訂を行なったデータとバージョン情報のみが設定された配布形式データ301とを管理センタ501に送信することもできる。管理センタ501の判定手段504はセンタデータベース505のデータと比較し、改訂版であるか否かを判断する。そして、改訂されたデータと判断したら、変換手段503は改訂されたデータに利用制限情報303を付加し、配布形式データ301を作成して再配布を行う。この場合、センタデータベース505に記録されている前回配布時のデータの利用制限情報303を基に、センタデータベース505に記録されている前回の配布情報と同一の利用者端末201に、同一の利用制限情報303を付加する。そして、センタデータベース505に改訂記録を保存する。

#### 【0068】

しかしながら、上記の方法で改訂されたデータの配布を行なうと、実施の形態1と同様、利用者端末201から他の利用者端末Aに再配布されたデータに対しては、改訂されたデータの配布が行なわれないことになる。そこで、管理センタ501で再配布の記録を管理する。利用者端末201は実施の形態1と同様に再配布情報を生成する。再配布情報は変換手段211により署名が行なわれ、管理センタ501の公開鍵5で暗号化される。

## 【0069】

暗号化された再配布情報は通信手段202により管理センタ501へ送信される。これには、利用制限情報303に加えたセンタの連絡先を用いる。データ作成者端末401の変換手段404は暗号化された配布情報を管理センタ501の秘密鍵5により復号し、判定手段405が利用者端末201の署名を確認する。管理センタ501の判定手段504が正規の利用者端末201からの送信であると判断すれば、センタデータベース通信手段506を介して再配布情報をセンタデータベース505に記録する。

## 【0070】

更に、利用者端末Aが利用者端末Bに配布形式データ301の再々配布を行なう際にも、同様にして配布記録データベース105を更新できる。以上により、管理センタ501は、配布形式データ301が何重に再配布されても、改訂データの配布毎にセンタデータベース505を更新することができる。こうして全ての配布形式データ301の保持者に対して改訂されたデータを配布することができる。

## 【0071】

以上で説明した各実施の形態のデータ配布システムは、利用者ごとに利用条件を設定するシステムであるが、例えば、社内でのデータ配布に用いることも可能である。この場合は、利用者ごとに利用条件を設定するのではなく、例えば課長職以上に同条件で全員配布を行うという利用形式にしてもよい。この場合、利用者である課長職以上の社員が、専用のパスワードや社員番号の入力等を利用者情報入力手段207から行なうことで、配付されたデータを利用できる。この場合、利用制限情報303の変更は、例えば課長に配布されたデータを部下に対して

再配布する際に、設定されたコピー数では足りなくなつたため、コピー可能数を増やしたいといった場合に用いられる。

#### 【0072】

なお、各実施の形態における記憶媒体203は持ち運び可能としてもよく、例えば携帯型メモリなどがあてはまる。この場合、利用者は利用者端末Aで使用しているメモリ（記憶媒体）をそのまま利用者端末Bで使用することができる。この場合、メモリに保存されているデータに対する利用制限は、利用者端末A、利用者端末Bのいずれにおいても同様となる。

#### 【0073】

なお、通信手段として、インターネットやイントラネット等による伝送、データ蓄積が可能なデバイスの移動が考えられる。更に、各実施の形態におけるデータベースは、データ蓄積が可能な装置全般を含み、HDD、フレキシブルディスク、携帯型メモリカード、CD-R、DVD-RAMなどがこれに当たる。

#### 【0074】

##### 【発明の効果】

以上のように本発明によれば、配布を行ないたいデータに対して、データ作成者端末で利用条件を詳細に設定し、利用者端末へデータを送信することが可能となる。さらに利用者側では、データ作成者端末に対して利用条件の変更要求を行なうことが可能であり、データ配布端末は変更要求の内容を確認して、変更を許可することができる。

#### 【0075】

さらに、データ配布を管理する管理センタを設けることにより、データ配布の記録を一箇所で管理することが可能となり、この場合もデータ配布端末で利用条件の変更要求を確認することができる。

#### 【0076】

さらに、配布時に利用者端末ごとに表示領域の設定を行なうことで、配布時に元データを毎回加工することなく、利用者端末での表示領域の制限ができる。

#### 【0077】

また、利用者端末側で利用者により利用制限情報として時間情報を付加可能と

することで、データを第3者に盗難された場合にデータの漏洩を防ぐことができる。

【図8】

さらに、一度配布したデータを改訂した場合に、バージョン情報を設定するだけで、改訂後のデータを改訂前と同様の条件で利用者端末に改訂データを配布できる。

【図面の簡単な説明】

【図1】

本発明の実施の形態1のデータ配布システムに用いられるデータ作成者端末の構成図である。

【図2】

本発明の実施の形態1及び2のデータ配布システムに用いられる利用者端末の構成図である。

【図3】

実施の形態1及び2のデータ配布システムに用いられる配布形式データの説明図である。

【図4】

本発明の実施の形態2のデータ配布システムに用いられるデータ作成者端末の構成図である。

【図5】

実施の形態2のデータ配布システムに用いられる管理センタの構成図である。

【図6】

実施の形態2のデータ配布システムにおいて、利用制限情報変更要求の表示例である。

【図7】

実施の形態2のデータ配布システムにおいて、表示領域の制限例を示す説明図である。

【図8】

各実施の形態のデータ配布システムにおいて、変更要求リストの作成方法を示

す処理図である。

【図9】

従来のデータ配布システムにおいて、データ配布側と利用者側との処理手順を示す説明図である。

【符号の説明】

- 101, 401 データ作成者端末
- 102 データ作成手段
- 103 利用制限情報設定手段
- 104 第1の変換手段
- 105 配布記録データベース
- 106 配布記録データベース通信手段
- 107 第1の通信手段
- 108 第1の判定手段
- 109 ネットワーク
- 201 利用者端末
- 202 第2又は第5の通信手段
- 203 記憶媒体
- 204 記憶媒体インターフェース
- 205 利用制限情報取得手段
- 206 利用項目入力手段
- 207 利用者情報入力手段
- 208 第2又は第5の判定手段
- 209 利用処理手段
- 210 変更要求入力手段
- 211 第2又は第5の変換手段
- 212 利用制限情報書換手段
- 301 配布形式データ
- 302 データ情報
- 303 利用制限情報

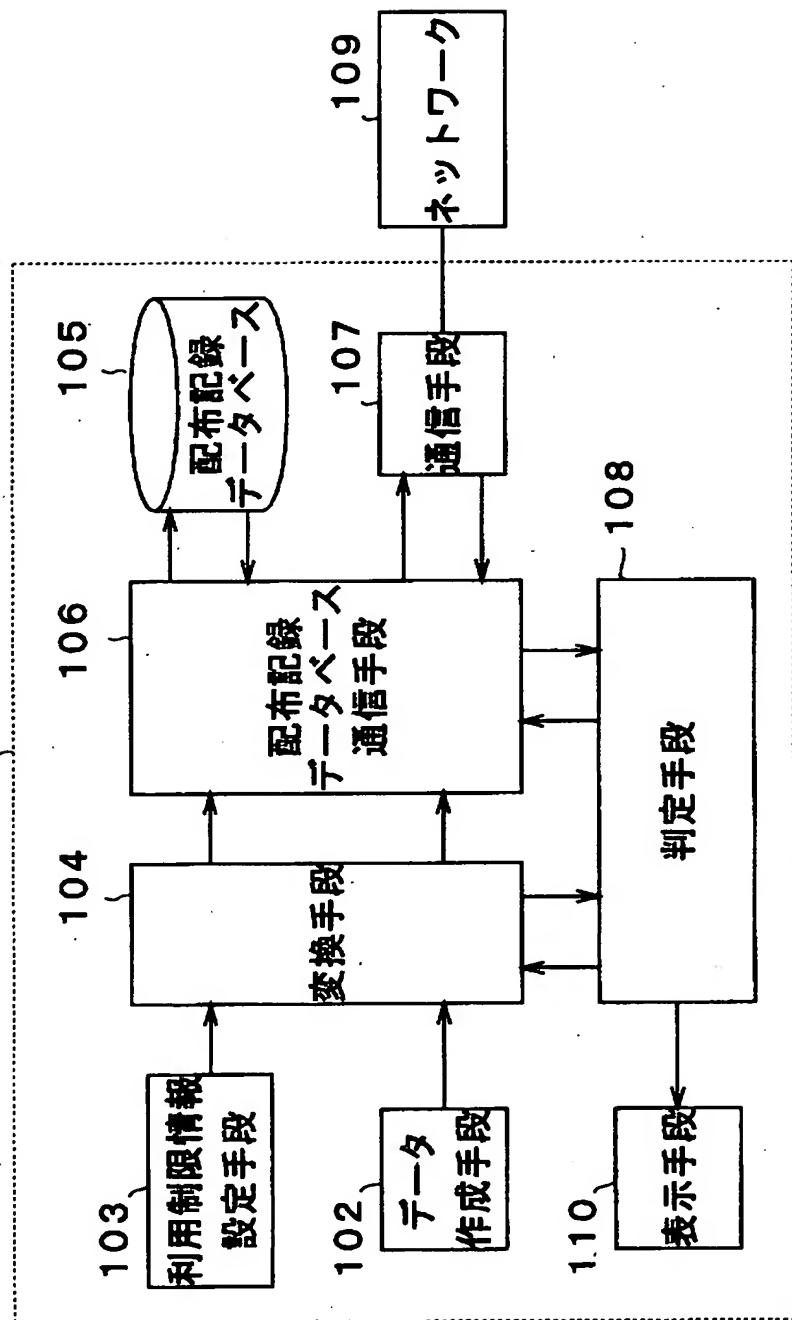
- 304 ハッシュ値
- 305 バージョン情報
- 306 コピー情報
- 307 配布先情報
- 308 データ暗号化鍵
- 309 コピー可能世代数及びコピー可能数
- 310 データ作成者公開鍵
- 311 作成者連絡先
- 312 利用制限
- 313 暗号化データ
- 314 プレーンテキスト
- 404 第3の変換手段
- 405 第3の判定手段
- 406 第3の通信手段
- 501 管理センタ
- 502 第4の通信手段
- 503 第4の変換手段
- 504 第4の判定手段
- 505 センタデータベース
- 506 センタデータベース通信手段
- 601 変更要求の表示内容
- 701 ウィンドウの大きさ
- 702 データの拡大率
- 703 非表示領域

【書類名】

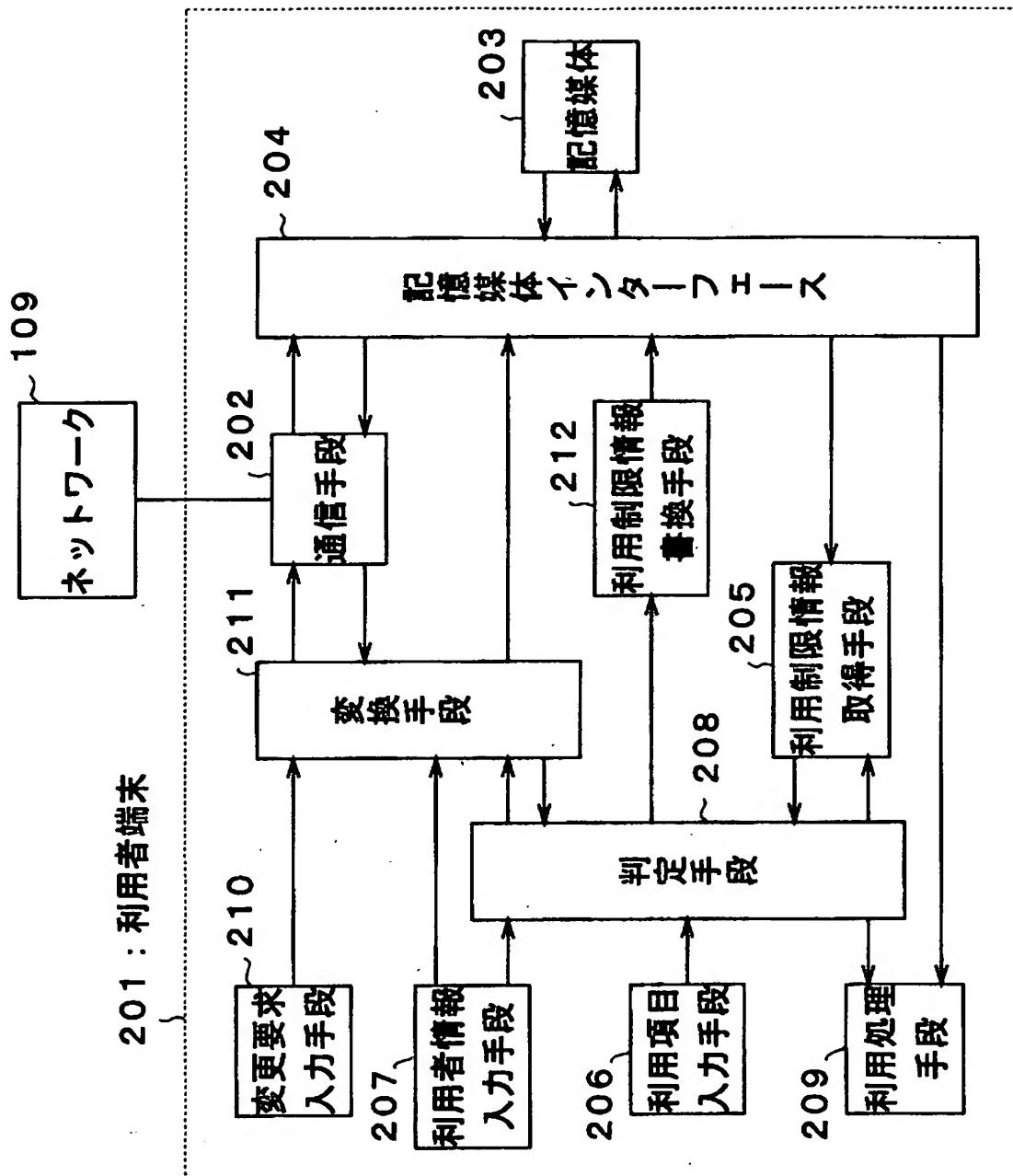
図面

【図1】

101：データ作成者端末

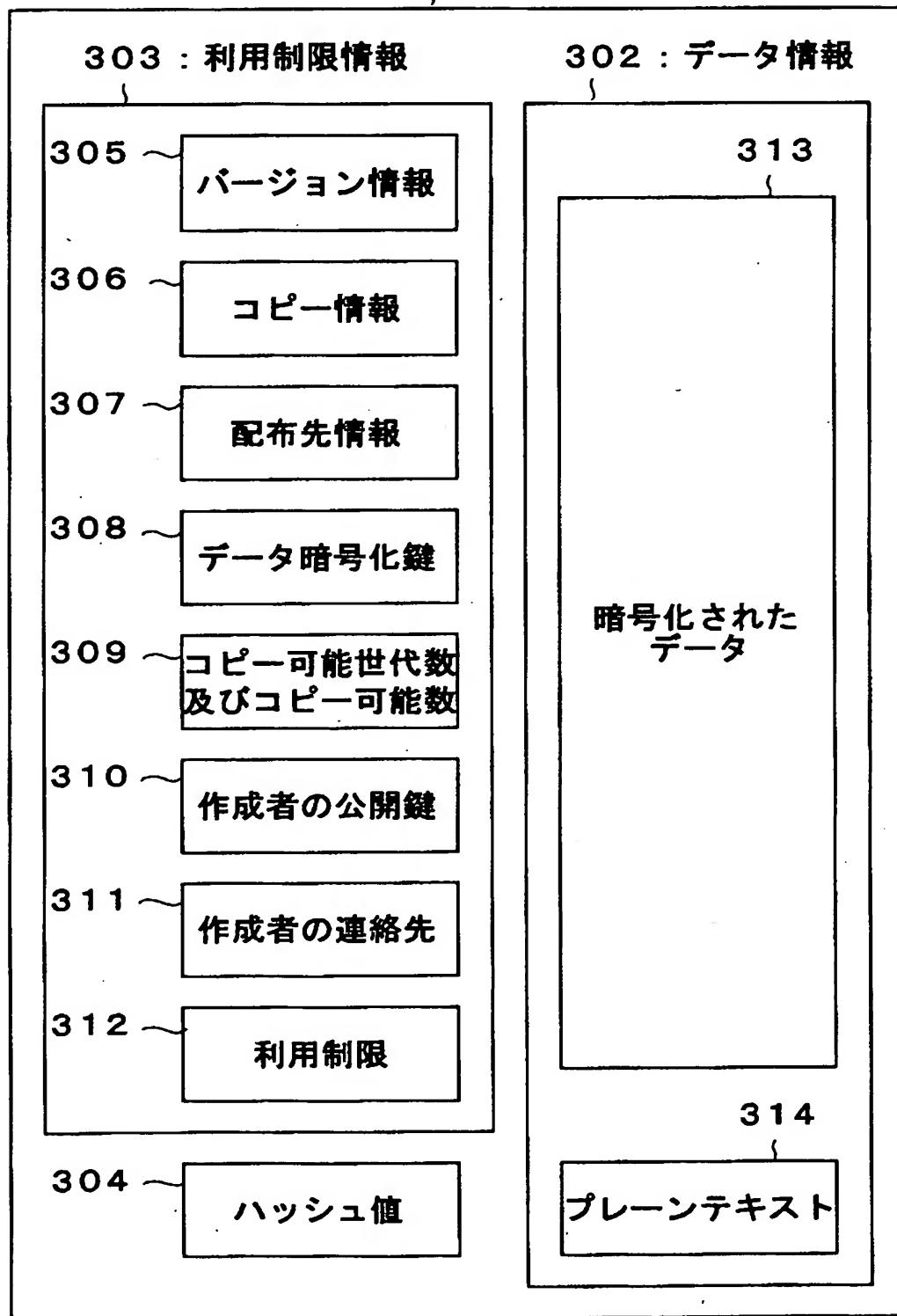


【図2】

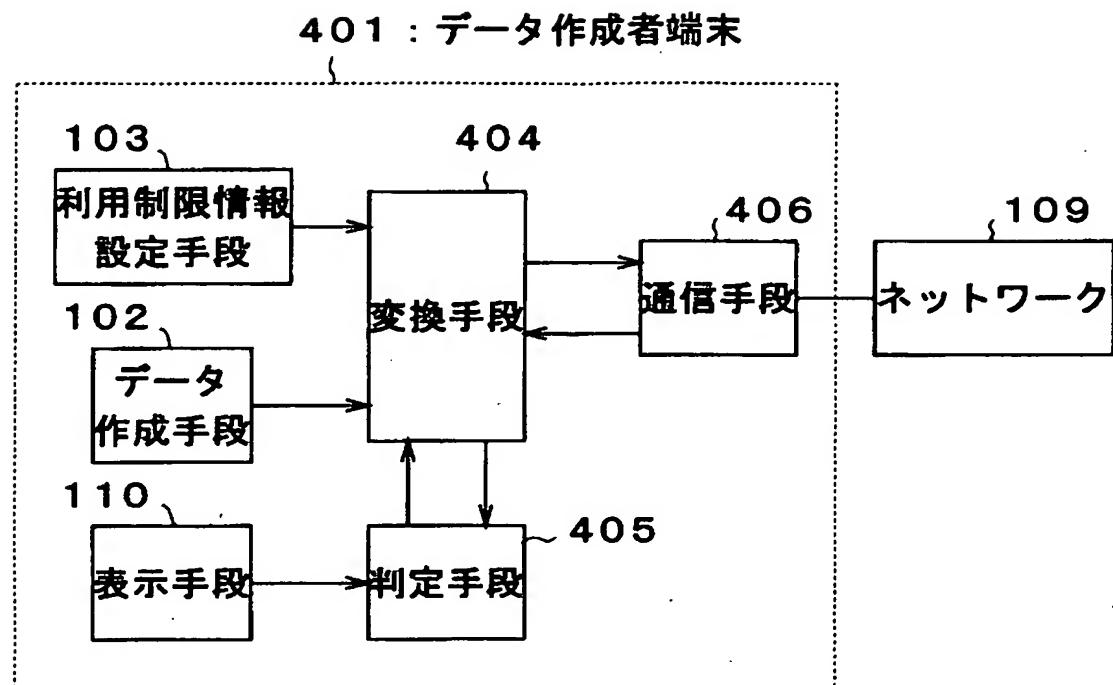


【図3】

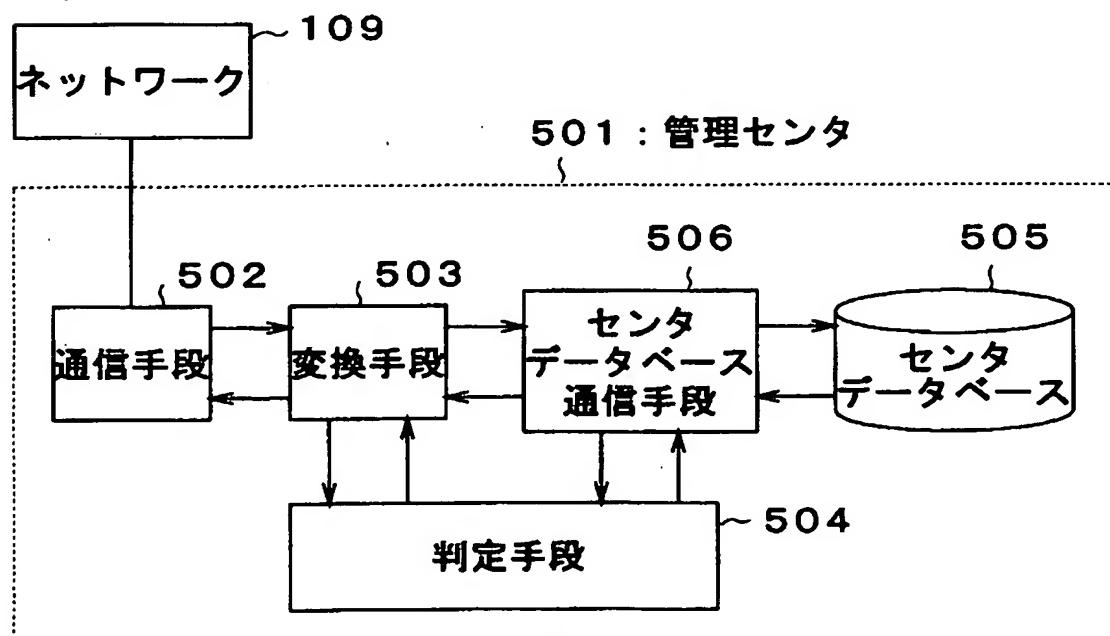
## 301：配布形式データ



【図4】



【図5】

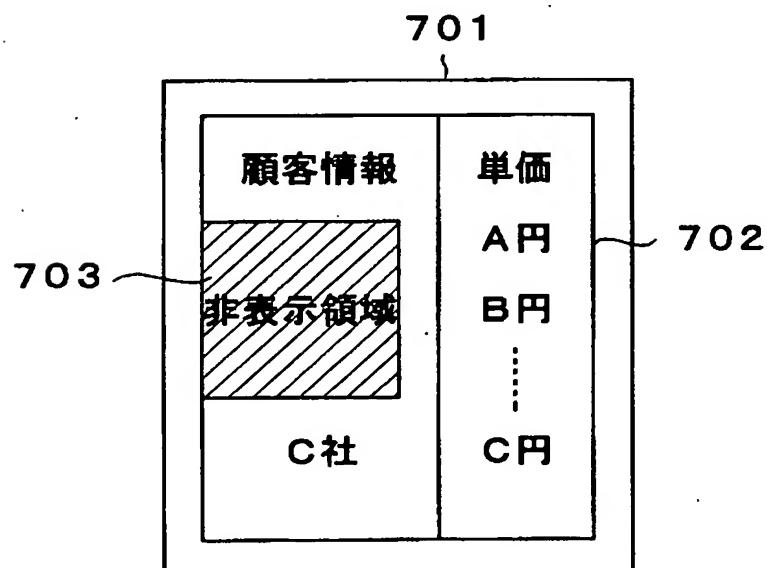


【図6】

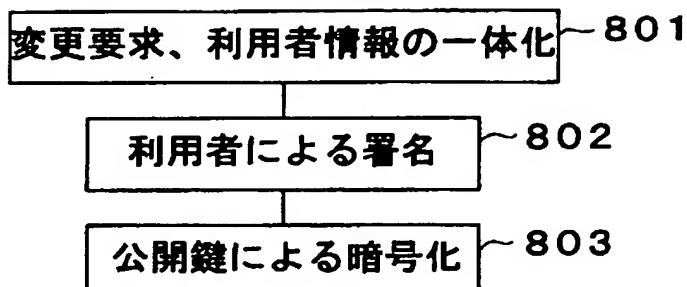
~ 601

配布者	× × × × ×		
項目	設定内容		変更要求
閲覧	可能		
プロト	許可	不可	許可
	世代数	—	1
	1	—	1
	2	—	

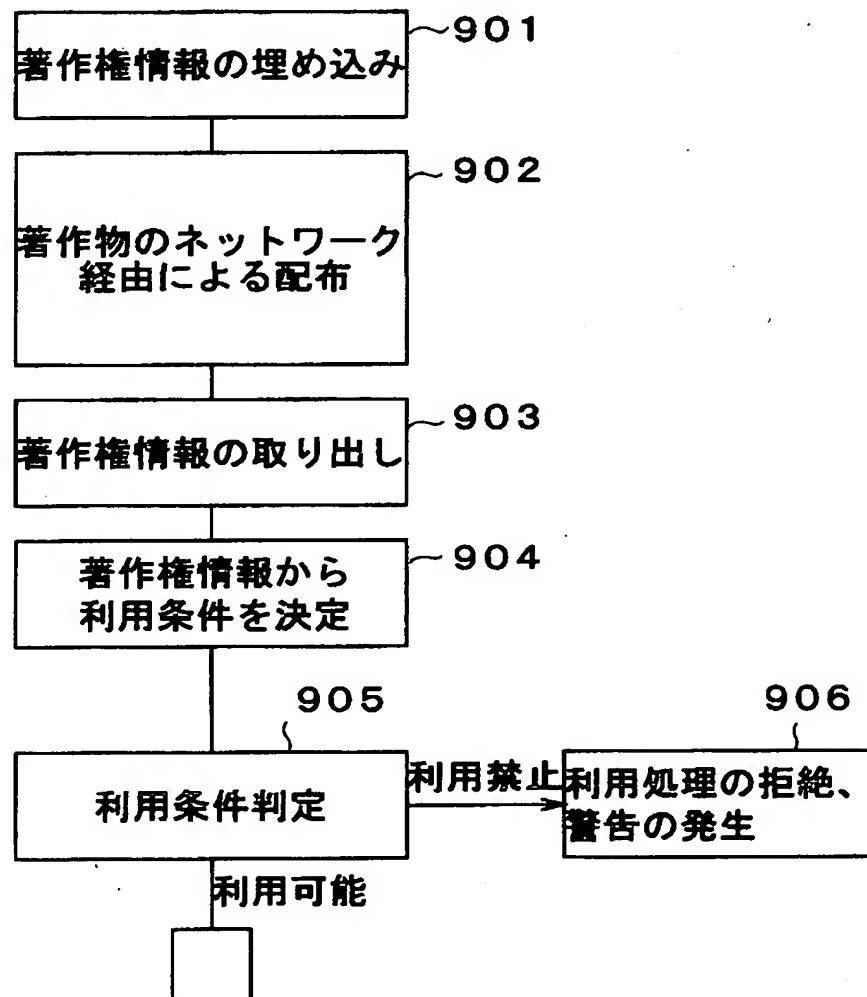
【図7】



【図8】



【図9】



【書類名】 要約書

【要約】

【課題】 データ配布を行なう際の著作権の保護方法、利用者に対する利用項目の制限方法において、利用者が設定された利用制限を正規の許可の下で変更可能にする機能を実現すること。

【解決手段】 データ配布システムの利用者端末201において、利用制限情報の変更要求入力手段210を設ける。変換手段211がその変更要求に署名と暗号化を行ない、通信手段202とネットワーク109を介してデータ作成者端末に送信する。データ作成者端末から利用制限情報の正規の書き換え許可を受け取ると、判定手段208が下した許可内容に従って、利用制限情報書換手段212が、変更された利用制限情報を記憶媒体インターフェース204を介して記憶媒体203に書き換える。

【選択図】 図2

認定・付加情報

特許出願の番号	特願2001-039489
受付番号	50100215050
書類名	特許願
担当官	第七担当上席 0096
作成日	平成13年 2月19日

<認定情報・付加情報>

【提出日】 平成13年 2月16日

次頁無

出願人履歴情報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社